REMARKS

Claims 1-4, 6-32 and 34-50 are now pending in the present application. Claims 1, 4, 6-9, 14, 16, 25, 28, 30, 31, 34, 40 and 47-49 have been amended, and Claims 5 and 33 have been cancelled, herewith. Reconsideration of the pending claims is respectfully requested.

I. 35 U.S.C. § 112, Second Paragraph

The Examiner rejected Claims 47-48 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter, which applicants regard as the invention. This rejection is respectfully traversed by amending such claims to correct a typographical error. Therefore, the rejection of Claims 47-48 under 35 U.S.C. § 112, second paragraph has been overcome.

II. 35 U.S.C. § 102, Anticipation

The Examiner rejected Claims 1-7, 9-13, 25-31, 33-37 and 49 under 35 U.S.C. § 102(b) as being anticipated by Duvall et al. (U.S. Patent No. 5,884,033) (hereinafter "Duvall"). This rejection is respectfully traversed.

With respect to Claim 1, Applicants have amended such claim to include features previously claimed in Claim 5 (which is thus being cancelled herewith without prejudice or disclaimer). As amended, Claim 1 recites "wherein the step of performing a corrective action comprises changing the destination of the outgoing transfer to the computer system" and "determining whether the program operates in response to the changed destination". As can be seen, Claim 1 is now directed to a specific technique for performing corrective action (if the destination for an outgoing transfer of data is not a trusted site), and specifically recites that *the destination gets changed* to instead be the computer system itself, and then determining whether the program (in this same computer system) which requested the outgoing transfer of data operates in response to this changed destination. In rejecting Claim 5 (whose features are now included in amended Claim 1), the Examiner states that Duval teaches (1) the feature of changing the destination of the outgoing transfer at column 4, lines 65-67, column 5, lines 1-29, and column 6, lines 20-26; and (2) the feature of determining whether the program operates in

response to the changed destination at column 4, lines 51-64 and column 5, lines 61-64. Applicants show error in such assertion as follows.

As to the claimed 'changing the destination' step recited in amended Claim 1, Duval describes at column 4, lines 65-67 whether to take an immediate or deferred action as a result of the retrieved filter, and does not in any way describe any change being made to the destination of an outgoing transfer of data. Duval describes at column 5, lines 1-29 that if either an immediate or deferred action is taken, a default action of either allowing or blocking the transmission can occur. This passage also describes the details of a deferred filter entry, such entry including a keyword such as a command, a filter pattern, a directional indicator for indicating incoming or outgoing transmissions to monitor, a compare directive for indicating the type of match required, and an action to be taken which is typically to allow or block the transmission. This passage ends by stating that if a match is found, the specified action in the filter is taken. This passage does not in any way describe *any change being made to the destination of an outgoing transfer of data*. As to the cited Duval passage at column 6, lines 20-26, such passage again describes a deferred action (in contrast to an immediate action), where if a match is made on an outgoing message, a deferred action is used to process subsequent incoming messages such as block or allow the incoming message. Again, this passage does not in any way describe *any change being made to the destination of an outgoing transfer of data*.

As to the claimed 'determining whether the program operates in response to the changed destination' step recited in amended Claim 1, since there is no teaching of a changed destination by Duval, it necessarily follows that there is no teaching of 'determining whether the program operates *in response to the changed destination*'. As to the passages cited by the Examiner in rejecting this determining step (as recited in originally filed Claim 5, and which is now recited in amended Claim 1), Duval describes at column 4, lines 51-64 either allowing or blocking a transmission, with a blocked message being provided to the user in the event of a block action. The message blocking is accomplished by *not executing the open command*, thus causing a failure result to be returned to the application which called the open command. There is no teaching of any changing of the destination of an outgoing transfer to the computer system, or any action occurring in response to such changed destination, such as determining whether the

program (which requested the outgoing transfer of data) operates in response to the changed destination. Rather, this passage merely teaches a failure to execute a command (the open command), and is then *responsive to this command failure*. As to the cited passage at Duval column 5, lines 61-64, such passage describes particular details of a deferred action, and in particular describes actions taken to *incoming* messages. Claim 1 is specific to *outgoing* transfer of data. Perhaps even more importantly, this cited Duval passage merely states that some incoming messages may be selectively blocked, with a corresponding blocked message being provided on the user screen to notify the user of the blocked action. Quite simply, selective blocking of an incoming message does not in any way teach or suggest changing the destination of an outgoing transfer of data, or any action being taken (specifically, determining whether the program operates) in response to such (missing) changed destination. Thus, Claim 5 is shown to have been erroneously rejected, and as Claim 1 has been amended herewith to include the features of originally filed Claim 5, it is shown that amended Claim 1 is not anticipated by the cited reference.

Applicants initially traverse the rejection of Claims 2-4 for reasons given above with respect to Claim 1 (of which Claims 2-4 depend upon).

Further with respect to Claim 4, Applicants urge that the cited reference does not teach the claimed feature of "wherein the corrective action comprises disabling the program". It should be noted that the program that is disabled is the program that requested the outgoing transfer of data. This claimed feature is particularly advantageous when malicious spyware is running in a computer system, as the spyware program that is attempting to transfer data out of the computer system is disabled. In rejecting Claim 4, the Examiner states that Duval teaches this claimed feature at column 4, lines 56-64. Applicants urge that this passage describes that a message is blocked ("by simply not executing the open command"), and an error message is returned to the application that initiated the open. Notably, the application that initiated the open is not disabled, but rather must maintain operability in order to receive and process such error message (such as displaying an error to a user display to notify the user). Thus, it is shown that this cited passage does not teach disabling the program that requested the outgoing transfer. Thus, Claim 4 is not anticipated by the cited reference as every element of the claimed invention is not identically or inherently shown in a single reference.

With respect to Claim 6 (and dependent Claim 7), such claim has been amended to be in independent form and has not been amended for purposes of patentability. Amended Claim 6 recites steps of "encrypting the data" and "determining whether the program operates in response to the encryption". Per the American Heritage® Dictionary of the English Language, Fourth Edition, published by Houghton Mifflin Company, decrypt means:

1. To put into code or cipher.

2. *Computer Science.* To alter (a file, for example) using a secret code so as to be unintelligible to unauthorized parties.

In rejecting Claim 6, the Examiner cites Duval column 5, lines 30-51 as teaching the claimed step of irreversibly decrypting, and Duval column 5, lines 61-64 as teaching the claimed step of determining whether the program operates in response to the encryption. Applicants urge that the passage cited by the Examiner at lines 30-51 of Duval column 5 . describes filter pattern matching of *incoming data* in response to a particular detected outgoing command being detected, where the *incoming data* can be discarded, replaced or edited. This is different from Claim 6 for several reasons. First, the passage describes altering *incoming data*, whereas Claim 6 is specifically directed to *outgoing data*. A teaching of one (processing of incoming data) does not teach the other (processing of outgoing data), as Duvall expressly states that the blocking actions that are available for an incoming message *are different from* those of outgoing messages (Duval column 5, lines 35-37). Perhaps more importantly, this passage does not in any way describe any encryption of data, as expressly recited in Claim 6. Quite simply, encrypting data is a particular type of data transformation, and a mere teaching of changing data (per Duval, the data is either discarded, replaced or edited) does not teach or otherwise suggest the specific claimed step of encrypting the data. Still further, this passage does not teach "determining whether the program operates *in response to the encryption*" (emphasis added). In rejecting this aspect to Claim 6, the Examiner cites Duval's teaching at column 5, lines 61-64. Noteworthy, this is the identical passage that was cited by the Examiner as teaching the claimed step of determining whether the program operates *in response to the changed destination*. So, according to the Examiner, the passage at

Duval column 5, lines 61-64 teaches *both* (1) determining whether the program operates in response to the changed destination, *and* (2) determining whether the program operates in response to the encryption. This simply is not the case. At column 5, lines 61-64, Duval states:

> "The system allows certain listed items in the response to an NNTP request to be blocked while allowing certain other strings. With these options, even though some items are allowed, a "Blocked" message should be provided on the user's screen to notify the user of the action taken."

As can be seen, this passage does not describe any determination being made as to whether a program operates, including whether the program operates in response to a changed destination or whether the program operates in response to the encryption of data. Rather, it describes selective blocking of incoming messages with an associated blocked message being provided to a user. Thus, Claim 6 (and dependent Claim 7) is further shown to have been erroneously rejected as there are further missing claimed features not taught by the cited reference.

Applicants initially traverse the rejection of Claims 9-13 for reasons given above with respect to Claim 1 (of which Claims 9-13 depend upon).

Further with respect to Claim 9 (and dependent Claim 10), Applicants urge that the cited reference does not teach the claimed steps of "determining whether the data includes personal information" and "performing a corrective action if the data includes personal information". It should be noted that the 'data' that is used in the determining step is with respect to a request for an outgoing transfer of data from a program in the computer system. In rejecting Claim 9, the Examiner states that the claimed personal information determination is taught by Duval at "column 7, lines 40-60; column 8, lines 8, lines 1-16". Applicants urge that this cited Duval passage at column 7 describes a technique for updating the filter database maintained within a client computer system by an update server, and is not in any way related to any determination with respect to outgoing data from a computer system, nor the determination of whether such outgoing data contains personal information. Rather, it describes an update procedure for updating filtering rules in a client's filter database. Nor does the cited Duval passage at column 8

overcome this teaching deficiency. Duval describes an ability of a user to edit the filter database containing the filtering criteria. There is no teaching of any determination of whether outgoing data contains personal information, as expressly recited in Claim 9. Thus, Claim 9 (and dependent Claim 10) is not anticipated by the cited reference.

Still further with respect to Claim 9 (and Claim 10), since there is no teaching of any determination of whether the data contains personal information, it necessarily follows that the cited reference does not teach any step of "performing a corrective action *if the data includes personal information*". The passages cited by the Examiner in rejecting this aspect to Claim 9 are the same passages cited by the Examiner in rejecting the personal information determination step of Claim 9. Again, these passages are with respect to updating and editing of the filter database itself, and are not with respect to any type of corrective action being performed based on data (which was requested to be transferred out of the computer system) that includes personal information. Rather, they describe ways to maintain the filter database itself, and do not describe use of the database in filtering content, and in particular do not describe performing a corrective action *if the data includes personal information*. Thus, Claim 9 (and Claim 10) is further shown to not be anticipated by the cited reference.

Still further with respect to Claim 9, the cited reference does not teach the synergistic combination of steps (1) determining whether the destination is a trusted site, and (2) determining whether the data includes personal information. While not admitting that either of these steps is known individually, Applicants show that "[w]hen determining the patentability of a claimed invention which combines two known elements, 'the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.'" *See In re Beattie*, 974 F.2d 1309, 1311-12, 24 USPQ2d 1040, 1042 (Fed. Cir. 1992) (quoting *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1462, 221 USPQ 481, 488 (Fed. Cir. 1984)). Thus, even assuming arguendo that each of these steps was individually known (which Applicants do not admit), it is still shown that there is nothing in the cited art to suggest any desire to combine such elements together, and thus Claim 9 would not have been obvious in view of the cited art.

Further with respect to Claim 11, such claim recites a feature of "wherein the step of performing a corrective action comprises storing a log of the outgoing transfer". In rejecting this claim, the Examiner cites Duval column 8, lines 1-62. Applicants urge that there, Duval describes two completely different aspects of his system – an editing manager that allows the user to edit the filter database (column 8, lines 1-16), and an alternate embodiment of the overall filtering scheme where the filtering is done by a server instead of by a client (column 8, lines 18-61). Other than being two aspects of Duval's overall system, these passages are not otherwise related – one describes a user action in a client and the other describes a system action in a server. Importantly, neither passage describes the logging of the outgoing transfer (of data). The first passage describes editing filtering rules, and is not concerned with any outgoing transfer of data, or the logging of such outgoing transfer. The second passage describes that the filtering database is maintained on a server system instead of a client system, and describes alternate filter matching techniques that are more appropriate for a server, but is not concerned with any logging of an outgoing transfer. At best, this cited passage teaches "The filter pattern is then stored in the probe table according to that least likely character combination". This storing of a filter pattern is not germane to any type of storing or logging of an outgoing transfer, as expressly recited in Claim 11. Thus, Claim 11 (and dependent Claims 12-13) is not anticipated by the cited reference.

With respect to Claim 25, Applicants have amended such claim to include features previously claimed in Claim 33 (which is thus being cancelled herewith without prejudice or disclaimer). As amended, Claim 25 recites "means for determining whether the destination is a trusted site" and "means for determining whether the data includes personal information". In addition, Claim 25 recites "means for performing a corrective action if the data includes personal information". Applicants urge that the cited reference does not teach all of these claimed features in combination (both a trusted site determination and a personal information determination). Further, the cited reference does not teach the personal information determination feature and resulting action for similar reasons to those further reasons specifically described above with respect to Claim 9. Thus, it is shown that amended Claim 25 is not anticipated by the cited reference.

Applicants initially traverse the rejection of Claims 26-31 for reasons given above with respect to Claim 25 (of which Claims 26-31 depend upon).

Further with respect to Claim 28, Applicants traverse for similar reasons to those given above with respect to Claim 4.

Further with respect to Claim 29, Applicants traverse for similar reasons to those given above with respect to Claim 1 regarding changing the destination of the outgoing transfer and determining whether the program (which requested the transfer) operates in response to the changed destination.

Further with respect to Claims 30 and 31, Applicants traverse for similar reasons to those given above with respect to Claim 6.

Applicants traverse the rejection of Claim 34 for reasons given above with respect to Claim 25 (of which Claim 34 depends upon).

Applicants traverse the rejection of Claims 35-37 for similar reasons to those further reasons given above specifically with respect to Claim 11.

Applicants traverse the rejection of Claim 49 for similar reasons to those given above with respect to Claim 25.

Therefore, the rejection of Claims 1-7, 9-13, 25-31, 33-37 and 49 under 35 U.S.C. § 102(b) has been overcome.

III.   35 U.S.C. § 103, Obviousness

The Examiner rejected Claims 8, 14-24, 32, 38-48 and 50 under 35 U.S.C. § 103(a) as being unpatentable over Duvall in view of Lin et al. (U.S. Patent No. 6,751,668) (hereinafter "Lin"). This rejection is respectfully traversed.

With respect to Claim 8, such claim has merely been amended to be in independent form and has not been amended for purposes of patentability. Amended Claim 8 recites steps of "determining whether the amount of data for the outgoing transfer is uncharacteristically high" and "performing a corrective action if the amount of data is uncharacteristically high". It should be noted that the determining step is with respect to the amount of data for the *outgoing transfer* (as requested by the program in the computer system). In rejecting Claim 8, the Examiner states that such determination is taught by Lin at column 2, lines 25-33 and 43-55. Applicants urge that Lin describes

how to combat a denial of service attack, where a computer system is being bombarded with *incoming messages* (Lin column 1, lines 14-25). The passage cited by the Examiner in rejecting Claim 8 is directed to a technique for limiting the rate of *incoming packets* to a computer system. Such incoming rate limit is different from Claim 8 for several reasons. First, the rate limit is with respect to *incoming* packets, whereas Claim 8 is specifically directed to an *outgoing* transfer of data. Secondly, the *rate of receipt* of incoming session establishment packets is the mechanism used to trigger the rate limitation. In contrast, Claim 8 specifically recites a determination is made as to the *amount of data for a given outgoing transfer* is uncharacteristically high. Quite simply, a rate of receiving commands (which is not based on the actual amount of data for such commands), as taught by Lin, is very different from an amount of data for a particular outgoing transfer of data, as claimed. For example, per Lin, packets one (1) byte in length may be received at a rate of 1,000,000 packets for second. Alternatively, per Lin, packets 1,000,000 bytes in length may be received at a rate of one (1) per second. The first Lin scenario would likely invoke the blocking of incoming session requests as the rate of receiving such requests is extremely high. However, the second scenario would likely not invoke the blocking of incoming session requests as the rate of receiving such requests is extremely low. The amount of data associated with a particular transfer of data is independent of a rate of receiving command packets, and thus Lin's teaching of selective passing of *incoming* requests based on the *rate of receiving* such requests does not teach the claimed feature of "determining whether the *amount of data for the outgoing transfer* is uncharacteristically high". In addition, because Lin is concerned with denial of service attacks – which are based on a rate of receiving session request packets, and is not based on the amount of data associated with such session request packets – there is no suggestion or other motivation to modify the teachings of Lin in accordance with the invention recited in Claim 8. Thus, it is shown that Claim 8 is not obvious in view of the cited references, as there is no suggestion or other motivation to modify the teachings of the cited references in accordance with the claimed invention.

Applicants traverse the rejection of Claim 14 (and dependent Claims 15-24), 38 (and dependent Claims 39-48) and 50 for similar reasons to those given above with respect to Claim 8.

Applicants further traverse the rejection of Claim 16 and 40 for similar reasons to the further reasons given above with respect to Claim 4.

Applicants further traverse the rejection of Claims 17 and 41 for similar reasons to the further reasons given above with respect to Claim 1.

Applicants further traverse the rejection of Claims 18, 19, 42 and 43 for similar reasons to the further reasons given above with respect to Claim 6.

Applicants further traverse the rejection of Claims 20, 21, 44 and 45 for similar reasons to the further reasons given above with respect to Claim 9.

Applicants further traverse the rejection of Claims 22-24 and 46-48 for similar reasons to the further reasons given above with respect to Claim 11.

Applicants initially traverse the rejection of Claim 32 for similar reasons to those given above with respect to Claim 25 (of which Claim 32 depends upon), and urge that none of the cited references teach or suggest the claimed personal information determination feature. Applicants further traverse the rejection of Claim 32 for similar reasons to those given above with respect to Claims 8 and 9.

Therefore, the rejection of Claims 8, 14-24, 32, 38-48 and 50 under 35 U.S.C. § 103(a) has been overcome.
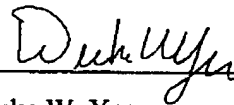
IV.   Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: _3/16/05_

Respectfully submitted,

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicants